

PATENT COOPERATION TREATY

To:

YOU ME PATENT & LAW FIRM
Seolim Bldg.
649-10
Yoksam-dong, Kangnam-ku
135-080 Seoul
Republic of Korea

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

Date of mailing (day/month/year)	8 August 2005 (08.08.2005)
-------------------------------------	----------------------------

Applicant's or agent's file reference OPP043359KR
--

FOR FURTHER ACTION See paragraph 2 below

International application No. PCT/KR 2005/000128	International filing date (day/month/year) 14 January 2005 (14.01.2005)	Priority Date (day/month/year) 14 January 2004 (14.01.2004)
---	--	--

International Patent Classification (IPC) or both national classification and IPC G06F 17/60, G07F 19/00, H04Q 7/38
--

Applicant

KTFREETEL CO., LTD.

1. This opinion contains indications relating to the following items:

- ☒ Cont. No. I Basis of the opinion
- ☐ Cont. No. II Priority
- ☐ Cont. No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Cont. No. IV Lack of unity of invention
- ☒ Cont. No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Cont. No. VI Certain documents cited
- ☒ Cont. No. VII Certain defects in the international application
- ☒ Cont. No. VIII Certain observations on the international application

2. FURTHER ACTION

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ AT Austrian Patent Office Dresdner Straße 87, A-1200 Vienna Facsimile No. +43 / 1 / 534 24 / 535	Authorized officer LOIBNER K. Telephone No. +43 / 1 / 534 24 / 323
---	--

IAP11 Rec'd PCT/PTO 14 JUL 2006

Continuation No. I

Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of the international application in the language in which it was filed.

Continuation No. V

Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims 2, 5-7, 10, 13, 14	YES
	Claims 1, 3, 4, 8, 9, 11, 12, 15, 16	NO
Inventive step (IS)	Claims ---	YES
	Claims 1-16	NO
Industrial applicability (IA)	Claims 1-16	YES
	Claims ---	NO

2. Citations and explanations:

The following documents have been cited in the Search Report:

D1: US2003/0191721A1
D2: WO1999/044114A1
D3: US2002/0198849A1

Document D1, which is considered to represent the closest prior art, discloses in line with the essential features of independent claim 1 and corresponding independent claim 12, an electronic transaction system being connected to a transaction terminal and a certification mobile terminal through a network (*cf. Figs. 2, 4, paragraph [0022]*) wherein said system comprises a server (200) including a software and data package having a business application (210), a signature correlation servlet (220), and a table (300) consisting of identification records of users/business having authorization to access said business application, wherein said business application is a core of a commercial-like site a user wants to deal with, wherein said business application is used to enable the user to approve the commercial transaction when being satisfied with the contents and the objects of the transaction (*cf. Figs. 2, 4, paragraph [0022]*). In order to approve a commercial transaction made by the user with his transaction terminal (110), the business application (210) uses the table (300) (*cf. Fig. 3, paragraph [0028]*) to retrieve an identification record (340) of the user and to look up the telephone number (320) of the mobile terminal (140) which is assigned to the user. Thereafter the business application (210) formats the transaction data and the

servlet (220) sends said data with a signature request to the mobile terminal (110) (*cf. Fig. 2, paragraph [0030]*). The mobile terminal (110) receives said signature request and the smart card (155) of the mobile terminal (110) checks the generated transaction content and prompts the user to validate the transaction (*cf. Fig. 2, stage S142*), whereby the transaction may be displayed on the screen (160) of the mobile terminal (140) in order to enable the user to review the content of the transaction received with the signature request (*cf. Fig. 2, paragraph [0010]*). Then the smart card (155) requests the user to enter a personal identification number (PIN) using the keyboard (150) of the mobile terminal (140) and upon receipt of the said identification the smart card signs the transaction using the user's private key (*cf. Fig. 2, stage S144*) and thereafter the signed transaction data are sent back to the servlet (220). The business application (210) performs a checking step in server (200) utilizing the public key (330) contained in the identification record (340) of the user to verify the signed transaction data (*cf. paragraph [0033]*). Furthermore, according to document D1 it is also suggested to utilize a Certificate Authority (CA) for issuing certificates by a trusted third party (*cf. paragraph [0024]*).

Considering this known prior art the essential features of independent claims 1 and corresponding independent claim 12 are not new, as the essential steps performed and functionality provided by the transaction processor, the message sender, the transaction history sender, the certifier and the service provider according to the subject matter of independent claims 1 and 12 is identical to the essential steps performed and functionality provided by the known server of document D1 including a software and data package having a business application, a signature correlation servlet, and a table.

Moreover, the Wireless Application Protocol (WAP) is used to transmit the signature request to the mobile terminal (*cf. paragraph [0022]*). It is however obvious to the skilled artisan that instead of using the Wireless Application Protocol (WAP) alternatively the short message service (SMS) or multimedia messaging service (MMS) can be utilized.

In conclusion, for the above reasons the subject matter of independent claims 1 and 12 and the additional features of dependent claims 3, 4 and 14 are not new as the same features have already been employed for the same reason in document D1. Furthermore, the additional features introduced in dependent claim 2 and 5 are directed to further design details which are either suggested by document D1 or obvious to the skilled person.

The subject matter of independent claim 6 and the additional features introduced in dependent claim 10 does not involve an inventive step in view of document D1 for the following reasons: According to the preferred embodiment disclosed in document D1 an asymmetrical cryptosystem is used, whereby at the mobile terminal the secret key of the user is employed when signing the transaction data and at the server the public key of the user is utilized to verify authenticity the signature. Said asymmetrical cryptosystem is employed providing the features of mutual authentication and non-repudiation of origin by optionally signing the transaction content at the server using the public key of the user and optionally a private key of the server (*cf. paragraph [0031]*). It is therefore considered, that the certificate used by the certification mobile terminal according to the subject matter of independent claim 6 is equivalent to the usage of public and private keys at the server and the certification mobile terminal according to document D1. The terminal according to document D1 does not provide a dedicated digital signature processor, however, the cryptographic processor in the smart card is equivalently used instead.

~~The subject matter of independent claim 7 and corresponding independent claim 12 differs~~
from the disclosure of document D1 in that the certification mobile terminal provides an additional interface for direct communicating with the transaction terminal, allowing the transaction history being directly received from the transaction terminal and responsively, the digitally signed transaction history is directly transmitted to the transaction terminal, preferably according to an infrared communication method.

However, a direct communication between a transaction terminal and a corresponding mobile telephone for providing authentication of said transaction has already been employed for the same reason in a similar authentication apparatus according to document D2 (*cf. Fig. 2, page 21, lines 18-25*).

Therefore, when combining the teaching of both documents D1 and D2 the subject matter of independent claims 7 and corresponding independent claim 12 does not involve an inventive step.

Document 3 describes in line with the subject matter of claims 15 and 16 a method for transacting with an off-line service providing system including a vending machine (*cf. Fig. 1, paragraph [0033]*) which comprises the following steps:

- selecting one of the transactions provided by the service providing system (*cf. Fig. 2, paragraph [0051]*);
- signing a stored digital certificate at the certification mobile terminal and transmitting the signed digital certificate to the service providing system according to an infrared communication method (*cf. paragraphs [0044]-[0047]*);
- providing the service at the service providing system according to the selected transaction when the user is certified using the previously received signed digital certificate (*cf. paragraphs [0048]*);

Considering document D3, the subject-matter of claims 15 and 16 is completely anticipated and therefore not new.

With respect to document D3 also the subject-matter of independent claim 8 in combination with the subject matter of dependent claims 9 and 11, which is directed to a corresponding certification mobile terminal which is specifically configured to perform the essential steps of the already known method according to the subject of claims 15 and 16, is likewise not new, because the special technical features of said certification mobile terminal have already been employed for the same purpose in the cellular network terminal (*cf. Fig. 3, paragraph [0045], [0054]-[0057]*) according to document D3.

In conclusion, in view of document D1 the subject matter of independent claims 1 and 12 is not novel and the subject matter of independent claim 6 is not inventive. The subject matter of independent claims 7 and 13 does not involve an inventive step when considering documents D1 and D2 in combination. The subject matter of independent claims 8 and 15 is not new in view of document D3.

Furthermore, dependent claims 2-5, 9-11, 14 and 16 do not contain any additional feature which in combination with the features of any claim to which they refer involve an inventive step for the reason that the subject matter of said claims is either in principle directly derivable from the disclosure of documents D1 or D3, or is suggested in combination of documents D1 and D2 or represent simple design details which are generally known to a person skilled in the art.

Industrial applicability is given.

Continuation No. VII:

Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

In order to meet the requirements of Rule 6.3 (b) PCT, whenever appropriate, each independent claim should be clearly delimited in relation to the closest prior art (for example D1) using the two-part form.

In order to meet the requirements of Rule 5.1 (a)(ii) PCT document D1 to D3, which disclose prior art that is relevant to the present invention, should be cited in the description and the said relevant prior art should be briefly outlined.

Reference signs in parentheses should be inserted in the claims to increase their intelligibility. This applies to both the preamble and the characterizing portion (see Rule 6.2 (b) PCT).

Continuation No. VIII:

Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

The applicant is kindly informed, that, occasionally, throughout the description and the claims some words appearing at the end of a line are truncated and wrapped over to the beginning of the following line, see for instance the last word in the third line of paragraph [4] of the description and the third line of claim 3.

From the description it becomes clear that the transaction history is received from the transaction terminal and thereafter the signed transaction history is transmitted to the transaction terminal. However, according to claim 11 the interface transmits the transaction history. It is assumed that the signed transaction history is meant.

Therefore, claim 11 lacks clarity and should be amended accordingly.

There is an unnecessary proliferation of independent claims identified and the various definitions of the invention given in independent system claim 1, in independent apparatus claims 6, 7 and 8 and corresponding method claims 12, 13 and 15 are such that the claims as a whole are not clear and concise, contrary to Article 6 PCT.

Therefore, the claims should be recast to include only the minimum necessary number of independent claims in any one category (Rule 6.4(a)-(c) PCT).

In the present case it is considered appropriate to use at least only one independent claim in any category.

When amending the application the applicant should be aware that the claims in the various categories are linked by a single general inventive concept and to avoid giving raise to further objections by inadvertent addition of subject matter.

PATENT COOPERATION TREATY

WO 2005/067402
PCT/KR2005/000128

PPOT

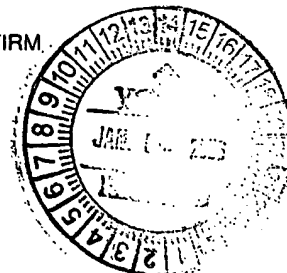
From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING
TRANSMITTAL OF COPY OF INTERNATIONAL
APPLICATION AS PUBLISHED OR REPUBLISHED

To:

YOU ME PATENT & LAW FIRM
Seolim Bldg.
649-10
Yoksam-dong, Kangnam-ku
Seoul 135-080
RÉPUBLIQUE DE CORÉE



Date of mailing (day/month/year)
22 December 2005 (22.12.2005)

Applicant's or agent's file reference
OPP043359KR

IMPORTANT NOTICE

International application No.
PCT/KR2005/000128

International filing date (day/month/year)
14 January 2005 (14.01.2005)

Priority date (day/month/year)
14 January 2004 (14.01.2004)

Applicant
KTFREETEL CO., LTD. et al

The International Bureau transmits herewith the following documents:

- ☐ copy of the international application as published by the International Bureau on under No. WO
- ☒ copy of international application as republished by the International Bureau on 22 December 2005 (22.12.2005) under No. WO 2005/067402
For an explanation as to the reason for this republication of the international application, reference is made to INID codes (15), (48) or (88) (as the case may be) on the front page of the attached document.

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Authorized officer

Philippe Becamel

Facsimile No.+41 22 740 14 35

Facsimile No.+41 22 338 70 90

Form PCT/IB/311 (January 2004)

BEST AVAILABLE COPY